Commentaire de la proposition de directive européeenne relative à la protection des données à caractère personnel (1ère partie)

Boulanger, Marie-Helene; de Terwangne , Cécile

Published in:
Cahiers Lamy du Droit de l'Informatique

Publication date:
1992

Document Version
le PDF de l'éditeur

Commentaire de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (1re partie)

I. – Objet de la directive

Sur le territoire de l'Europe communautaire peuvent désormais circuler, chaque jour plus librement, les biens et marchandises, les capitaux, les services, les personnes. Sous-jacente et indispensable à ces mouvements, la libre circulation de l'information (1) s'est révélée être un complément incontournable des libertés fondamentales mises en place par le Traité de Rome (2) ; complément dont la réalisation est ressentie chaque jour davantage comme une nécessité (3).

Qu'il s'agisse, en effet, d'acheter un bien par correspondance au-delà d'une frontière, d'effectuer un paiement à l'étranger, de regrouper au sein de la société-mère les données concernant le personnel de ses filiales implantées dans d'autres Etats membres, d'échanger des informations policières lors d'enquêtes judiciaires ou administratives menées à l'échelle de plusieurs pays ou lors de poursuites au-delà d'un territoire national, ou qu'il s'agisse encore de transmettre des données médicales en cas de soins assurés à l'étranger, le même phénomène de flux transfrontières de l'information apparaît à la base de chaque opération.

Mais est également à envisager une seconde réalité : l'information peut être considérée comme un bien en soi et constituer l'objet même de l'échange (banques de données commerciales, fichiers de marketing, activité de "chasseurs de têtes", ...). La volonté de créer un marché de l'information prend ici le pas sur la nécessité du mouvement de l'information.

Dans les deux cas, le désir de voir les données circuler sans entraves au sein de la Communauté doit s'accompagner de la prise en compte scrupuleuse des libertés individuelles en jeu. C'est essentiellement la vie privée des individus qui est en cause. Cette notion doit être comprise dans son acception la plus large. Il ne s'agit pas, en effet, de vouloir préserver pour chacun un monde secret dont il a seul la clef, conception à laquelle la plupart opposent un « je n'ai rien à cacher, moi ». Ce qu'il faut tendre à protéger, c'est l'autonomie de l'individu, la maîtrise que celui-ci doit conserver de « l'image informationnelle » qui circule à son propos (4).

Ainsi que l'a fait remarquer le Parlement européen dès 1982, la Communauté se doit donc de « pallier les effets secondaires de ses activités (économiques et commerciales) » (5).

Il ne faut toutefois pas tomber dans l'excès d'une stratégie défensive qui conduirait à renier le progrès technologique et non à le maîtriser. Pareil excès déduirait du droit de l'individu de disposer pleinement de ses données, la faculté de s'opposer de façon discrétionnaire à toute utilisation de celles-ci. Un tel réflexe procéderait d'une vision partielle de la nature des données. En effet, pour individuelle qu'elle soit, la donnée peut être vue sous l'angle de la collectivité, et devient dès lors information. En tant que telle, elle est appelée à circuler librement au nom de l'article 10 de la Convention européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales (6). Ainsi, la Cour constitutionnelle fédérale allemande a affirmé, dans une décision désormais de principe portant sur la loi fédérale relative au recensement de la population, que *« l'information, même si elle a trait à une personne, reflète une image de la réalité sociale qui ne peut être imputée exclusivement à la personne concernée. (...). L'individu doit donc, en vertu d'un intérêt général prépondérant, accepter en principe que des restrictions soient apportées à son droit à l'autodétermination en matière d'information »*.

Dans cette optique, le Professeur Knaub propose de considérer qu'« une donnée personnelle ne méritera d'être protégée que dans la mesure où il est admis que la société n'est pas à même de faire un usage légitime de cette donnée et que, partant, celle-ci peut et doit lui être cachée » (7).

Cependant, fonder la possibilité d'utilisation ou, à l'inverse, de secret d'une donnée sur la base de la légitimité du besoin social est insuffisant. Une telle analyse n'apporte pas de réponse adéquate aux situations, combien fréquentes, dans lesquelles l'intérêt de la société à voir circuler l'information est parfaitement légitime, mais le désir de l'individu de retenir son information par devers lui l'est tout autant. C'est alors d'une délicate mise en balance que sortira la solution. Il ne sera plus question seulement d'intérêt « légitime » mais bien d'intérêt « prépondérant » de la société à connaître l'information sur celui de l'individu à ne pas la voir circuler (8).

Le défi en cette matière consiste donc à trouver un juste équilibre entre les besoins de la société et la protection de la liberté de l'individu. Semblable équilibre est l'expression d'un choix politique – traduit au sein d'une législation appropriée – effectué par les citoyens auxquels il appartient de fixer les limites du « degré de transparence de la personne » (9). Ce choix doit donc prendre place aux niveaux où le politique a tout son sens, car proche du citoyen. Cela explique et justifie les réglementations nationales divergentes, tout en soulevant la question de la pertinence d'une action communautaire.

Si l'on veut toutefois voir la libre circulation des données réalisée et s'instaurer un véritable marché européen de l'information, il faut nécessairement viser à l'harmonisation des différents régimes nationaux.

Une première tentative de favoriser les flux d'informations mettant en cause des individus (données à caractère personnel) tout en assurant à ceux-ci la protection de leur image informationnelle, la maîtrise et le contrôle de l'information qui les concerne, a vu le jour sous l'égide du Conseil de l'Europe. Il s'agit de la Convention 108 de 1981 (10). Dix ans après le vote de ce texte, il faut toutefois constater avec regrets que la réalité n'a pas suivi les intentions. Ainsi, si la convention a été signée par la plupart des Etats membres du Conseil de l'Europe ou, à tout le moins, de la Communauté européenne, nombreux sont encore les Etats qui se sont limités à ce geste et n'ont pas ratifié la convention. N'ayant pas, par le biais d'une norme nationale, intégré dans leur ordre juridique interne les règles contenues dans le texte, ces Etats privent non seulement leurs citoyens d'une protection effective, invocable devant les tribunaux, mais ils privent aussi les utilisateurs des données d'un code des règles à suivre pour exercer légitimement le traitement des informations.

D'autre part, il apparaît clairement aujourd'hui que la Convention 108 ne peut fournir à elle seule un cadre uniforme suffisant pour éviter les distorsions dans le fonctionnement du marché intérieur (11). Ce texte énonce en effet des principes généraux qui laissent une large place aux divergences d'interprétation et dès lors d'application. Ces divergences portent tant sur le champ d'application des législations nationales prises à la lumière des règles posées par la Convention (12) que sur les conditions qui entourent le traitement des données à caractère personnel (13), sur les exceptions admises ou sur les dispositions en matière de flux transfrontières.

Ces lacunes ou différences sont à la source d'un déséquilibre préjudiciable entre Etats membres, environnement propice à la création de « paradis de données ». Cela conduit en outre à des distorsions de concurrence sur le marché des services de traitement et de diffusion de l'information et entrave la mise en oeuvre des principes de liberté posés par le Traité de Rome (14).

Une volonté d'harmonisation a peu à peu vu le jour. L'initiative en revint à la Commission européenne, qui a émis en septembre 1990 une proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (15).

Ce texte vise à traduire de façon plus précise les principes généraux contenus dans la Convention du Conseil de l'Europe afin de garantir une réelle équivalence des pratiques en matière de protection des données dans les pays membres et de permettre à ces derniers d'adopter une approche commune face aux pays tiers. La philosophie de la directive diffère de celle qui anime la Convention de 1981. En effet, alors que celle-ci s'inscrit dans une perspective de protection des droits individuels, celle-là est orientée vers une dynamique d'échange et de marché de l'information (16).

(1) Par « information », il faut entendre au sens de notre analyse toutes « données à caractère personnel », c'est-à-dire « toute(s) information(s) concernant une personne physique identifiée ou identifiable » (article 2a de la directive).

(2) Article 8a du traité C.E.E.

(3) 2e et 4e considérants de la proposition de directive.

(4) C'est la Cour fédérale allemande qui, la première, tira de la protection constitutionnelle du droit à l'épanouissement de la personnalité, le « droit à l'autodétermination informationnelle » (recht auf « informationelle Selbstbestimmung »; 15 décembre 1983, BVerfGE 65, 1).

(5) Résolution du 5 mars 1982 relative à la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'information, *J.O.C.E.* n° C 87 du 5 avril 1982, p. 30 Rapport Sieglerschmidt, doc.1-598/81.

(6) L'article 10 de la convention européenne des droits de l'homme précise que « toute personne a droit a la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière... »

(7) G. Naub, « La protection des données », Conférence de Strasbourg : Droits de l'homme et Communauté européenne : vers 1992 et au-delà, 20 et 21 novembre 1989, SEC(89)8510-FR., p. 5.

(8) Voir *infra*, les différentes solutions du projet de directive lorsque deux intérêts légitimes contradictoires sont en présence.

(9) G. Knaub, *op cit.*, p. 6.

(10) Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg, le 28 janvier 1981.

(11) P.V. Petrucci, « Protection des données personnelles et marché des services de l'information » 38e rencontre annuelle du Comité d'Administration publique de l'Union de l'Europe occidentale, Bruges, 18-20 octobre 1989, p. 5.

(12) On citera comme exemples le fait que certains Etats incluent les fichiers manuels dans le champ de leur législation tandis que d'autres n'envisagent que les fichiers automatisés. Certains étendent la protection aux personnes morales, alors que la plupart la limitent aux personnes physiques.

(13) Certaines législations optent pour un régime de déclaration préalable du fichier; d'autres, pour un régime d'autorisation.

(14) P.V. Petrucci, *op cit.*, p. 3.

(15) Document COM. (90) 314 final - SYN 287 (13 septembre 1990).

(16) 6e considérant de la proposition de directive : « ... pour éliminer les obstacles à la circulation des données à caractère personnel le niveau de protection de la vie privée à l'égard des traitements de ces données doit être équivalent dans tous les Etats membres ».

Le but avoué est d'éviter que les exigences de protection des données ne puissent entraver les mouvements transfrontières sur le territoire de la Communauté (article 1, paragraphe 2 de la directive). A l'inverse de la Convention 108 qui laisse une porte (légèrement) ouverte aux Etats parties pour faire obstacle au principe de libre circulation des données personnelles (17), la directive interdit formellement les restrictions entre Etats membres au nom de la protection des données.

Aucune des libertés mises en place au sein de la Communauté européenne n'est absolue. Toutes connaissent des exceptions, justifiées notamment par l'intérêt général (18). Que la libre circulation des informations soit considérée comme une application particulière du principe de libre circulation des biens ou qu'elle soit rattachée à la libre prestation des services, elle est soumise, elle aussi, aux limites posées par l'intérêt général. La volonté présente derrière la directive est d'empêcher que chacun puisse à sa guise invoquer la protection de la « privacy » comme motif d'intérêt général pour mettre fin aux mouvements de l'information. L'ensemble du texte est l'expression de la prise en compte des limitations légitimes que l'on peut apporter à une liberté: la liberté de l'information, au nom d'une autre: la protection de la vie privée. Par le fait même que la directive pondère, avec un souci permanent d'équité, les intérêts en présence, il ne peut plus y avoir lieu à de nouvelles restrictions. Cela permet en outre de ne pas soumettre à l'interprétation de la Cour de Justice de Luxembourg la recherche de l'équilibre idéal entre deux libertés *a priori* contradictoires.

Il est toutefois à noter qu'un tel système présuppose l'existence d'un niveau équivalent de protection au sein de la Communauté. Or, l'article 28 de la directive envisage, en son deuxième paragraphe, que de « sérieuses divergences » (19) puissent être constatées entre la législation ou la pratique des Etats membres en matière de protection des données à caractère personnel. Cela semble donc contradictoire. Dans l'hypothèse où l'équivalence n'est pas acquise, un Etat se verrait-il en droit de freiner les échanges avec les pays moins protecteurs ? Le principe de libre-circulation de l'information serait par là mis en péril.

En fait, la directive ne précise d'aucune manière ce que peut faire l'Etat qui constate une situation de sérieuse divergence. Il devrait dès lors être fait référence, dès l'article premier posant le principe de la liberté des flux (article 1.2), à l'éventualité de divergences dont fait écho l'article 28. Dans une telle situation, l'obligation de liberté tombe et l'Etat redevient juge de l'opportunité d'autoriser ou de prohiber l'échange des données. Mais cela affaiblirait d'emblée la position de la directive par l'aveu que l'harmonisation pourrait ne pas être réalisée.

On peut, par ailleurs, préférer à l'interdiction pure et simple de l'article 1.2. une solution qui oblige l'Etat à faire constater l'inégalité de protection par les autorités de contrôle instituées à l'article 28 (20), avant d'être autorisé à restreindre les flux de données.

Enfin, il est évidemment possible de réduire la marge laissée aux Etats pour la mise en application dans leur ordre juridique interne de certaines dispositions du texte. Si des divergences sérieuses demeurent encore, elles ne pourront plus dès lors que découler du non-respect de la directive par un Etat membre, situation conduisant à l'application de sanctions.

II. – Champ d'application de la directive

A. – Données à caractère personnel

Avant d'attacher notre propos à commenter les règles essentielles mises en place par la proposition de directive pour organiser l'exercice légitime des activités de fichage, il nous faut préciser la notion centrale de « données à caractère personnel » (21), clef de la protection communautaire.

La définition retenue par la proposition de directive est identique à celle déjà adoptée par la Convention 108 du Conseil de l'Europe, définition par ailleurs présente en termes similaires dans de nombreuses législations nationales. Entre donc dans le champ de la directive « toute information concernant une personne physique identifiée ou identifiable » (22). Le texte poursuit en apportant des précisions sur ce qu'il faut entendre par individu identifiable. Bien que l'illustration soit donnée dans des termes peu ouverts (« personne qui peut être identifiée par référence à un numéro d'identification ou une *information similaire* »), on peut considérer que toute méthode d'identification doit être prise en compte.

(17) L'article 12.3 de la Convention prévoit deux possibilités de dérogation au principe de liberté des flux : d'une part lorsque la législation d'un Etat prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données (données sensibles) ou de ces fichiers, et que la réglementation de l'autre Etat partie n'apporte pas de protection équivalente (1 2.3.a) ; d'autre part lorsqu'un transfert de données est projeté vers le territoire d'un autre Etat contractant, mais ce dernier pays ne servant que de lieu de transit vers un Etat tiers à la Convention, procédé qui permettrait de contourner la législation du pays d'origine (12.3.).

(18) *Cf.* articles 56 et 66 du Traité de Rome.

(19) Le deuxième alinéa de l'article 28 stipule que « si le Groupe de protection des données à caractère personnel constate que de sérieuses divergences s'établissent entre la législation ou la pratique de Etats membres en matière de protection des données à caractère personnel, divergences qui risquent de porter atteinte à l'équivalence de la protection dans la Communauté, il en informe la Commission ».

(20) Voir *infra* pour le détail des autorités en question.

(21) On trouve aussi, principalement dans les textes législatifs et la pratique française, la notion de « données nominatives ».

(22) Article 2.a.de la proposition de directive.

En toute logique, tout ce qui n'est pas donnée à caractère personnel est donnée anonyme et est hors du champ de la directive. La définition de l'« anonymisation » permet ainsi de circonscrire par l'extérieur la notion de donnée personnelle.

Au sens de la directive, la donnée anonyme est celle qui ne peut plus être reliée à une personne physique déterminée ou déterminable, « ou moyennant seulement un effort excessif en personnes, en frais et en temps » (23). Tant que les efforts consentis pour identifier un individu auquel rattacher des données ne sont pas excessifs, ces données seront donc considérées comme « à caractère personnel », l'individu étant identifiable (24).

La référence à un effort excessif soulève de nombreuses réactions au sein des milieux concernés. Elle prend cependant en compte le fait que les données ne sont pas anonymes une fois pour toutes mais peuvent éventuellement être repersonnalisées. Toutefois, le caractère excessif est relatif et doit s'apprécier en fonction des moyens dont dispose le détenteur des données. Ainsi des données qui seraient anonymes pour une administration qui n'a pas les moyens techniques ou financiers de les rattacher à des individus (efforts excessifs), pourraient donc être librement transférées à une entreprise. Or, pour celle-ci, les efforts à fournir ne seront peut-être pas excessifs au vu de l'importance de ses moyens. Les données, anonymes au départ, doivent être alors à nouveau couvertes par la protection.

B. – Fichiers

Le champ d'application de la directive est défini par référence à la notion de « fichier » (25) : « *les Etats membres appliquent les dispositions de la présente directive aux fichiers du secteur privé et du secteur public à l'exclusion des fichiers du secteur public dont les activités ne relèvent pas du champ d'application du droit communautaire* ».

Le maintien de la notion de fichier – dépassée pour d'aucuns – est totalement pertinent d'un point de vue formel, dans la mesure où il offre une base matérielle pour les formalités administratives. Utilisée généralement à bon escient dans la directive, cette notion recouvre l'objet d'un certain nombre de procédures administratives (notification du fichier, déclaration du fichier, ...) qui poseraient des problèmes de mise en œuvre si elles devaient être effectuées sur la base des traitements (26).

Notons ici qu'à l'exemple de la majorité des législations européennes en vigueur ou en voie de le devenir, les auteurs du projet de directive entendent soumettre les fichiers manuels aux règles protectrices.

Cette extension est pertinente car, si les dangers inhérents au fichage ont été exacerbés par le recours à l'outil informatique, il ne faut cependant pas fonder la protection de la vie privée sur le support de l'information touchant à l'individu. Une distinction en fonction de la nature du support serait malheureuse dans la mesure où il s'agirait d'une prime au refus de l'évolution technologique. En outre, les progrès réalisés dans la technique du scanning rendent la distinction entre fichiers manuels et fichiers automatiques de plus en plus théorique puisque les données contenues dans un fichier manuel peuvent aisément faire l'objet de traitements automatisés. Enfin, il ne faut pas négliger le risque réel de fuites, de contournements, de la réglementation par le biais de fichiers (manuels) refuges.

Ayant tiré les enseignements des deux générations de législations qui sont apparues en Europe en matière de protection des données, les auteurs de la proposition de directive ont non seulement élargi le champ du texte en ne le limitant pas aux seuls fichiers automatisés, mais ils ont par ailleurs soustrait de l'application des règles communautaires certaines catégories de fichiers.

Ainsi, les fichiers tenus à des fins privées et personnelles ne sont pas concernés. Il s'agit, par exemple, d'un carnet d'adresses privé – qu'il soit manuscrit ou incorporé dans un ordinateur – ou de fichiers utilisés en vue de gérer la vie ou l'« administration » familiale. Le carnet d'adresses professionnel, par contre, n'échappe pas aux conditions posées par la directive (27). Remarquons que seuls les fichiers détenus par des personnes physiques sont exemptés.

Font également l'objet d'une exception, les fichiers détenus par des associations sans but lucratif notamment à caractère politique, philosophique, religieux, culturel, syndical, sportif ou de loisir, pourvu qu'ils s'inscrivent dans le cadre de l'objectif légitime de ces associations, qu'ils ne se rapportent qu'aux seuls membres et correspondants de l'association et

(23) Article 2.b.de la proposition de directive.

(24) Cela conforte donc notre large interprétation de la notion d'individu « identifiable ».

(25) Par « fichier » il faut entendre, aux termes du projet de directive « tout ensemble de données à caractère personnel, centralisées ou réparties sur plusieurs sites, faisant l'objet d'un traitement automatisé ou qui, bien que ne le faisant pas, sont structurées et accessibles dans une collection organisée selon des critères déterminés de manière à faciliter l'utilisation ou l'interconnexion des données » (article 2.c.).

(26) Voy. projet de loi belge qui exige la déclaration de tout traitement (projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ch., sess. ord., 90-91, 6 mai 1991, 1610/1).

(27) Il connaît cependant un régime particulier dans la mesure où les données contenues proviennent de sources généralement accessibles au public et sont uniquement destinées à la correspondance : le consentement des personnes concernées n'est pas requis (article 8.1.b.) et le détenteur du carnet d'adresses ne doit pas informer les personnes reprises dans son carnet lorsqu'il transmet leur adresse à un tiers (article 9.2.).

qu'ils ne soient pas communiqués à des tiers (article 3.2.b.) (28). Cette exception est inspirée du privilège accordé initialement aux associations pour tenir les listes de leurs membres. Dans le texte de la directive, ce privilège a cependant été notablement étendu. Or, il faut savoir où tracer la limite entre la liberté d'association et les autres droits et libertés individuelles (notamment la protection de la vie privée, le droit d'accès à ses informations). En ce sens, les termes généraux de l'exemption de l'article 3.2.b. sont inadéquats: pourquoi ne pas lier les fichiers en question aux principes fondamentaux, garants de la légitimité des activités de fichage, à savoir principe de finalité, exigence de qualité des données, respect du droit d'accès des personnes concernées ?

III. – Légitimité des traitements de données

La directive couvre tant le secteur public que le secteur privé. Toutefois, les dispositions s'appliquant à l'un ou l'autre secteur diffèrent fortement. Avant de nous attarder à l'analyse des réglementations mises en place, il nous faut préciser la portée de la distinction effectuée par les auteurs du texte entre le secteur public et le secteur privé, et juger de la pertinence de pareille distinction.

A. – Distinction secteur public – secteur privé

Le critère adopté par la directive pour distinguer les deux secteurs est fondé, non pas sur la nature de l'organisation, de droit public ou de droit privé, des entités concernées, mais sur la fonction ou l'activité exercée (29). Ainsi, les organismes ou entités de droit privé qui participent à l'exercice de l'autorité publique ressortissent au secteur public (30), alors que les administrations, organisations et entités du secteur public qui exercent une activité commerciale ou industrielle relèvent du secteur privé (31).

La distinction opérée entre les deux secteurs ne se justifie pas tant par le fait que les fichiers du secteur public doivent être considérés comme *a priori* plus dangereux mais parce que la nature des fichiers tenus dans le secteur public exige des précautions et des modes de contrôle différents. Les fichiers publics se caractérisent en effet :

- par le fait qu'ils sont exhaustifs, c'est-à-dire qu'ils reprennent l'ensemble de la population ou la totalité d'une catégorie de citoyens;
- par leur mode de création qui relève d'une décision unilatérale contraignante issue de l'autorité publique, alors que le fondement d'un fichier du secteur privé est, dans la plupart des cas, à trouver dans une relation contractuelle libre entre le fiché et le ficheur.

Etant donné cette dernière caractéristique, la relation de soumission qui lie l'individu aux entités publiques, il faudrait logiquement inclure dans le secteur public les entreprises, organismes ou entités qui exercent une activité en situation de monopole. A cette fin, il suffirait de préciser que les entités exceptées du secteur public sont celles qui participent à une activité industrielle ou commerciale dans le champ concurrentiel. Le texte de la directive suivrait par là la nouvelle version de la loi fédérale allemande de protection des données, dernière née dans le panorama législatif européen, aux termes de laquelle les entreprises publiques qui prennent part à la concurrence sont soumises aux dispositions régissant le secteur privé, les entreprises qui bénéficient de monopole demeurant donc comprises dans le secteur public (32).

Une question reste à soulever avant d'étudier le régime propre à chaque secteur: qu'en est-il des situations dans lesquelles un organisme public poursuit une activité commerciale en marge de la mission d'intérêt public qu'il remplit ? Cette question se pose notamment face aux nombreux fichiers publics tenus à des fins de service public mais présentant un indéniable intérêt économique et étant dès lors susceptibles de faire ou faisant déjà l'objet d'une exploitation commerciale (fichiers de l'Institut National des Statistiques, Registre du commerce, Registre d'immatriculation, ...). La constitution de ces fichiers, s'inscrivant dans le cadre du service public à remplir, doit répondre aux conditions imposées à la création d'un fichier au sein du secteur public. La commercialisation en tant que telle implique, quant à elle, à la fois un changement de finalité (les fichiers en question n'ont certainement pas été mis en place à des fins commerciales) et la communication des données au secteur privé. Ces phénomènes sont chacun envisagés par la directive qui les assortit de différentes conditions dans le cadre du régime s'appliquant au secteur public.

B. – Régime du secteur public

Préférant centrer notre propos davantage sur le sort réservé par la directive au secteur privé, nous ne décrirons pas ici le régime appliqué au secteur public. Certaines réflexions peuvent cependant être émises.

Dans le cas de fichiers publics, le droit à l'information indispensable pour assurer un service public efficace s'appuie sur les principes constitutionnels de légalité, de proportionnalité et de spécialité.

Du respect de ces trois principes dans la matière qui nous occupe découlent deux conséquences majeures.

Tout d'abord, toute banque de données publique doit être créée sous le contrôle du pouvoir législatif. De façon générale, ce principe exige une certaine coordination et un contrôle des systèmes informationnels du secteur public. Il importe que le législateur puisse connaître à tout moment les circuits d'information existants ou projetés à l'intérieur des administrations. La question évoquée déborde largement celle des libertés individuelles. Il s'agit bien plutôt d'un problème d'équilibre des pouvoirs et donc de libertés publiques. En effet, l'utilisation croissante de l'information dans le secteur public renforce les pouvoirs d'action de l'exécutif central et, au sein de celui-ci, de certaines administrations. Cela modifie l'équilibre des pouvoirs, garant traditionnel de la démocratie. Il est donc important que le législatif, par le biais d'un organe de contrôle, puisse maîtriser le développement de l'information du secteur public.

Deuxièmement, le fait qu'un organisme public ne puisse enregistrer des données que dans le cadre de la mission qui lui a été confiée (principe de spécialité) et pour autant que cela lui est nécessaire (principe de proportionnalité) exige que la finalité de chaque banque de données publique soit clairement annoncée.

La directive ne tire pas les justes conclusions de ces observations. Ainsi elle autorise l'établissement de fichier ou le traitement de données personnelles pourvu que cela soit *« nécessaire pour l'exécution des missions de l'autorité publique »*. Nulle part n'est exigé que les missions confiées à l'autorité publique en cause le soient par ou en vertu d'une disposition légale. Nulle part n'est envisagé un examen, préalable à la mise en oeuvre des traitements importants ou sensibles, effectué par un organe de contrôle issu du législatif .

Par ailleurs, aux termes de l'article 5.1.b de la directive, le traitement de données pour une finalité différente de celle pour laquelle le fichier a été établi est autorisé si *« un intérêt légitime de la personne concernée ne s'oppose pas à ce changement de finalité »*. Cette formule revient à autoriser *a priori* des détournements de finalité sous réserve que le sujet des données prouve que son intérêt légitime en serait lésé.

C. – Régime du secteur privé

On observe une nette différence de niveau d'exigences entre le régime mis en place pour le secteur public et celui réservé au secteur privé.

1. Enregistrement de données dans un fichier - Traitement de données

Pierre d'angle de la protection communautaire, le consentement de la personne concernée doit être obtenu pour que le ficheur soit en droit d'enregistrer des données à caractère personnel et de les traiter (33).

La notion de consentement doit être entendue, au sens de la directive, comme consentement informé. Ce qui implique des conditions strictes concernant la validité de la volonté émise par la personne concernée. L'article 12 précise de la sorte que cette dernière, avant de marquer son accord, doit être informée des finalités du fichier, des types de données enregistrées, du type d'utilisation qui en sera faite, des destinataires éventuels des données et enfin des coordonnées du responsable du fichier.

Le consentement doit ensuite être spécifique et exprès et doit encore préciser les types de données, les formes de traitement et, le cas échéant, les destinataires qu'il couvre.

On l'aura compris, dans cette mesure, le principe du consentement préalable risque d'entraîner des formalités lourdes et contraignantes et de freiner considérablement nombre d'activités du secteur privé. Les auteurs de la directive ont été conscients de ce revers de la médaille d'une protection maximale basée sur la connaissance et la volonté de l'individu. Ils ont donc introduit d'importantes exceptions au principe du consentement préalable. Celles-ci méritent d'être passées ici en revue, avec la critique qu'elles suscitent. C'est de leur portée que dépendent à la fois l'effectivité de la protection et la praticabilité de la réglementation.

Une remarque essentielle doit toutefois être faite avant de nous attarder à décrire les situations dans lesquelles l'enregistrement et le traitement des données est légitime. Ces conditions doivent se lire de pair avec un principe fondamental, base de toute politique de protection des données: le principe de finalité. Déplorons que celui-ci n'apparaisse qu'à l'article 16 de la proposition de directive, alors que son importance capitale justifie une bien meilleure mise en exergue.

Avant toute chose, il faut donc savoir que les données ne peuvent être enregistrées que pour des finalités déterminées, n'être utilisées que de manière compatible avec ces finalités, et doivent être pertinentes, adéquates par rapport aux finalités (34).

Cela étant dit, quels sont les cas dans lesquels l'enregistrement et le traitement des données personnelles peuvent avoir lieu sans que le consentement de la personne concernée soit requis ?

(28) Les associations professionnelles organisées sous forme d'association sans but lucratif ne sont pas reprises dans la liste, alors que le pendant de telles associations, les organisations syndicales, est inclus dans l'énumération. Les associations entrent toutefois logiquement dans la catégorie exemptée (l'énumération n'est qu'exemplaire, *cf.* « notamment »).

(29) L'exposé des motifs est très clair à ce sujet: « ces définitions sont basées sur la nature du service fourni par les entités concernées, sans égard à leur statut public ou privé ». COM. (90) 314 final, p. 20.

(30) Voir aussi la version rafraîchie de la loi fédérale allemande de protection des données (Gesetz sur Fortenwicklung der Datenverarbeitung und des Datenschutzes, BDSG, du 20 décembre 1990) qui prévoit que quelle que soit sa nature, l'entité qui « prend en charge des missions de l'administration publique » doit être considérée comme relevant du secteur public.

(31) Article 2.g. et h. de la proposition de directive.

(32) BDSG § 12 et 27.

(33) Article 8.1. de la proposition de directive.

(34) Ce principe essentiel est posé dans la Convention 108 du Conseil de l'Europe (article 5 b et c) et se retrouve dans l'ensemble des législations nationales.

Sur cette question, le texte de la directive est très proche de la solution adoptée lors de la récente révision de la loi allemande de protection des données dont il a déjà été fait mention plus haut. La D S G (35) version 1990 reprend en effet comme situations de légitimité des traitements internes les mêmes trois hypothèses (notamment) que celles envisagées dans la directive. L'intérêt particulier de la référence à la loi allemande tient dans le fait que le législateur fédéral a pu intégrer dans ce texte les leçons de la plus longue tradition européenne en la matière, autant qu'il a pu tirer parti des évolutions de la pratique législative de ses voisins.

- Ainsi, le traitement est légitime s'il « *se situe dans le cadre d'un contrat ou d'une relation de confiance quasi-contractuelle, avec la personne concernée et est nécessaire à leur réalisation* » (36). A cette formule essentiellement centrée sur le lien contractuel entre le ficheur et le fiché, on eût pu préférer l'inspiration du modèle de certaines réglementations de la « deuxième génération » (37) qui prévoient une dispense de l'obligation d'informer le fiché dès l'instant où celui-ci devrait raisonnablement avoir connaissance de l'enregistrement de ses données. Cette solution, qui dans les textes législatifs nationaux en question ne vise pas la dispense de consentement mais la dispense de l'information de l'existence du fichage, est plus large que ce que recouvrent les termes de la directive. Par là-même, la primauté serait donnée à la praticabilité de la réglementation et à la circulation des informations.
- Il n'est pas besoin non plus du consentement des personnes concernées lorsque « les données proviennent des sources généralement accessibles au public et (que) leur traitement est uniquement destiné à la correspondance » (38). La formulation de la seconde partie de cette disposition laisse perplexe (cette proposition finale n'est pas présente dans le texte allemand). Faut-il voir dans la règle énoncée la disposition générale régissant les activités de marketing et de mailing ? Il eût mieux valu alors ne pas limiter le traitement des données envisagé aux seules fins de correspondance. L'ambiguïté peut dès lors être levée si au terme « correspondance » on substitue l'expression « à des fins de prospection commerciale ou publicitaire ».
- Enfin, le traitement est admis lorsque « *le responsable du fichier poursuit un intérêt légitime, à condition que l'intérêt de la personne concernée ne prévale pas* » (39). Flagrante soupape de secours au régime exigeant du consentement préalable, cette disposition, devrait garantir la praticabilité de la législation mise en place, mais risque par ailleurs d'être la source d'incertitudes nées de divergences d'interprétation et, partant, d'application.

La loi allemande précise que les intérêts de tiers ou l'intérêt public peuvent également être pris en considération pour autoriser l'utilisation ou la communication des données (40). Elargissement que l'on ne retrouve pas dans le texte communautaire, ce qui soulève quelques inquiétudes dans les milieux concernés.

Les hypothèses couvertes par le principe de l'obtention du consentement du sujet des données reviendront donc essentiellement pour le secteur privé – hormis le cas des données sensibles – aux traitements de données destinées à être communiquées à des tiers (hors du cadre des activités de prospection commerciale).

Il demeure que les formalités imposées pour recueillir le consentement (informé, spécifique, exprès et détaillé) sont lourdes. Ce n'est pas tant les renseignements à donner qui apparaissent contraignants que le fait que ce consentement spécifique et exprès (article 12 b) risque de poser des problèmes de gestion difficiles pour le ficheur qui devra tenir compte des desiderata propres à chaque fiché (41). En outre, le consentement de ce dernier peut être retiré à tout moment (article 1 2.c).

Dans cette mesure, un système d'information préalable au traitement, accompagné de la possibilité pour le fiché de demander le retrait de son nom du fichier, serait sans aucun doute moins lourd pour le ficheur. Cette formule de l'acceptation implicite à défaut de réaction ou d'objection tient par ailleurs davantage compte d'une réalité dans laquelle nombre des personnes concernées, qui ne donnent pas leur accord exprès, ne le refusent pas sur base d'une objection mais ne prennent tout simplement pas la peine de manifester leur volonté. Il est à noter que la directive contient déjà les éléments de ce système alternatif moins contraignant pour les entreprises tout en étant protecteur des intérêts essentiels des fichés. Ainsi, un droit de retrait est explicitement prévu à l'article 14.6 à propos des fichiers de prospection commerciale et publicitaire, et une obligation d'information préalable portant sur les mêmes renseignements que ceux prévus à l'article 12 s'impose lors de la communication des données à des tiers.

Les situations dans lesquelles le consentement du sujet n'est pas requis correspondront souvent à des situations dans lesquelles les données auront été collectées directement auprès de la personne concernée (dans le cadre d'un lien contractuel ou autre). Remarquons que dans cette hypothèse la directive prévoit l'obligation de fournir, lors de la collecte des données,

(35) Bundesdatenschutzgesetz, déjà citée.
(36) Article 8.1.a. de la directive; § 28 (1) 1 BDSG.
(37) Législations néerlandaise (wet persoonsregistratie du 28 décembre 1988, *Staatsblad*, 1988, p. 665) et belge (projet) notamment.
(38) Article 8.1.b. de la proposition de directive.
(39) Article 8.1.c. de la proposition de directive; § 28 (1) 2 BDSG.
(40) § 28 (2) 1.a.
(41) Par ailleurs, la question se pose de savoir si le consentement informé sera exigé lors de chaque modification de l'un des renseignements dont question à l'article 12 de la proposition de directive.

un ensemble d'informations englobant les informations prévues pour le consentement. La volonté éclairée du sujet des données est donc, par cet autre biais, préservée.

2. Communication des données

La directive est assez permissive quant aux conditions dans lesquelles les données personnelles peuvent être communiquées. Ainsi, la communication est en principe libre, pourvu qu'elle ne soit pas incompatible avec la finalité du fichier (c'est au ficheur qu'il revient de prouver la compatibilité) et qu'elle ne porte pas atteinte à l'ordre public.

La notion de « communication » n'est pas définie dans le texte de la directive. Communément entendu, il s'agit de la transmission des données à un tiers. Dans la mesure où la communication met donc en cause la notion-clef de « tiers », c'est en fait ce dernier terme qu'il faut cerner de façon précise.

Par « tiers » on peut entendre toute personne qui n'est pas sous l'autorité du responsable du fichier. Dans le cas de personnes morales, l'analyse de l'organisation juridique de ces personnes, critère clair et fiable, devrait permettre de déterminer si celui qui demande communication des données est soumis à l'autorité du responsable du fichier. Il y aurait dès lors communication lorsque des données sont transmises à un tiers, même si celui-ci est situé à l'intérieur de l'entreprise du maître du fichier. Par contre, il n'y aurait pas communication si le destinataire des données est un établissement géographiquement distinct mais sous l'autorité du même responsable. Bien sûr, il n'est pas question de considérer qu'il y a lieu à communication quand le tiers auquel les données sont transmises est le sujet des données lui-même ou la personne qui traite les données pour le compte du maître du fichier (service-bureau) .

Si la directive fait montre de souplesse en s'en remettant au principe de finalité pour juger de la pertinence et donc de l'admissibilité des transmissions de données, elle assortit néanmoins l'opération d'une formalité. L'article 9 prévoit en effet une obligation pour le responsable du fichier d'informer le fiché sur les caractéristiques de base du fichier, lors de la première communication des données ou en cas d'ouverture d'une possibilité d'accès on line.

Cette disposition vise en premier lieu les entreprises ayant pour objet social la communication à des tiers (agences commerciales de crédit, chasseurs de têtes, sociétés de vente par correspondance), entreprises qui seront systématiquement soumises à l'obligation d'information du fiché lors de la communication. En ce sens, la solution est identique à celle pratiquée en Allemagne (42). Au Danemark, c'est directement à l'enregistrement que l'agence de renseignements commerciaux doit avertir le fiché.

(42) § 3 (1) deuxième phrase BDSG.

Il semble que l'avertissement du fiché à l'enregistrement plutôt que lors de la communication soit administrativement plus simple à contrôler, à la fois du point de vue de l'entreprise et de celui de l'autorité de protection. Quand aura lieu la première communication ? Et surtout, n'eût-il pas été préférable que le fiché informé puisse, le cas échéant, rectifier certaines données avant qu'elles ne soient communiquées ?

Par ailleurs, alors que dans les pays cités (Allemagne, Danemark) la disposition est limitée aux entreprises ayant pour objet le traitement de données destinées à la communication, la proposition de directive évoque l'obligation d'information du fiché pour toute entreprise dès lors qu'elle communique une donnée. Tel est le cas par exemple d'une banque qui transmet certains renseignements à propos d'un client à un autre client. Sur ce point, l'article 9 risque de créer quelques difficultés. Ces entreprises seraient tenues de vérifier pour chaque communication que le fiché en soit dûment averti .

Une telle contrainte pour les entreprises travaillant pour compte propre (dans le cadre de relations contractuelles avec le fiché) apparaît disproportionnée. L'information donnée sur base de l'article 9 sera sans doute inutilement redondante avec les renseignements donnés au moment de la collecte des données (43) ou au moment où le consentement est recueilli (44) – d'autant que le fiché a une connaissance implicite du traitement opéré, étant donné les relations contractuelles (ou quasi-contractuelles) qu'il a nouées avec le maître du fichier. Or, cela n'est pas le cas pour les fichiers destinés à être communiqués à des tiers, qui devraient être seuls visés par la disposition.

Notons que la directive laisse la porte ouverte à des dérogations à l'obligation d'informer le fiché, si cette formalité s'avérerait impossible ou impliquant des efforts disproportionnés. Une exception est également admise lorsque la fourniture des informations heurte des intérêts légitimes prédominants du ficheur ou un intérêt d'égale valeur d'un tiers (45).

3. Notification à l'autorité de contrôle

La formalité de notification de l'établissement d'un fichier à l'autorité de contrôle nationale est l'objet de controverse.

Les entreprises du secteur privé y voient la source de charges administratives lourdes et onéreuses. Les organes de protection des données estiment par contre que la connaissance de l'existence des fichiers dès leur création est la condition *sine qua non* d'un

(43) L'article 18 prévoit que la personne auprès de qui les données sont collectées doit être informée (notamment) des finalités du fichier, des destinataires des informations, du nom et de l'adresse du responsable du fichier.
(44) Article 12 de la proposition de directive, *cf. supra*.
(45) Article 10 de la proposition de directive.

contrôle efficace. Pour les individus fichés, enfin, un registre exhaustif accessible au public constitue une source d'information qui leur permettra d'identifier les fichiers susceptibles de contenir des données les concernant.

La réalité est cependant différente. Là où des registres accessibles ont été mis en place, l'expérience a montré qu'ils ne sont pas consultés par le public. On peut dès lors s'interroger sur l'utilité d'un outil inutilisé. D'autre part, les obligations de notification ont donné naissance dans les pays qui les ont étendues à tous les fichiers, à des engorgements administratifs. Les énergies des organes nationaux de protection des données sont de la sorte monopolisées par des charges bureaucratiques au détriment des activités de contrôle. En outre, la formalité de notification est difficilement applicable aujourd'hui avec le développement fulgurant de la micro-informatique. Ainsi, des actes quotidiens tels « la composition d'une lettre (professionnelle) et son archivage (...), le stockage de numéros de téléphone (professionnels) sur une calculatrice de poche » (46) correspondent à la définition même du traitement des données à caractère personnel tel qu'envisagé dans la directive. « Il est impossible d'en tenir un registre centralisé » (47).

A cet égard, la solution adoptée dans le texte de la proposition de directive tient compte des tendances actuelles à la réduction du champ de la formalité de notification. Seuls, en effet, les fichiers de données destinées à être communiqués et ne provenant pas de sources publiques doivent faire l'objet d'une déclaration à l'autorité de contrôle (article 11). Cette disposition est inspirée des solutions allemande et danoise qui ne prescrivent de notification qu'aux entreprises traitant des données à des fins de communication (48).

En supprimant la formalité de notification pour les fichiers internes (fichiers généralement alimentés dans le cadre de relations avec les personnes concernées), c'est à l'individu fiché plus qu'à une autorité nationale de protection que l'on confie le soin de contrôler, pour ces fichiers, la pertinence et la qualité des données traitées. Quels sont donc les moyens d'action des personnes concernées ?

.....

(46) P. Petrucci « Protection des données personnelles et marché des services de l'information », 38e Rencontre annuelle du Comité d'administration publique de l'Union de l'Europe Occidentale. Bruges, 16-20 octobre 1989, p. 6.

(47) P. Petrucci, *Ibidem.*

(48) Notons que le FCRA américain prévoit également une obligation de notification pour les agences de renseignements commerciaux.

Marie-Hélène BOULANGER

et Cécile de TERWANGNE,

des *Facultés Universitaires Notre-Dame de la Paix (Namur),*

sous la direction d'Yves POULLET,

Directeur du Centre de Recherche Informatique et Droit (C.R.I.D.).